주성분 분석과 기계학습을 이용한 사물인터넷 공격 탐지

이지구[O], 이수진(교신저자)[*]
[O]국방대학교 국방과학학과,
[*]국방대학교 국방과학학과
e-mail: jglee0120@gmail.com[O], cyberkma@gmail.com[*]

IoT Attack Detection Using PCA and Machine Learning

Ji-Gu Lee[O], Soo-Jin Lee(Corresponding Author)[*]
[O]Dept. of Defence Science, Korea National Defense University,
[*]Dept. of Defence Science, Korea National Defense University

● 요 약 ●

최근 IoT 환경에서 기계학습을 이용한 공격 탐지 모델의 연구가 활발히 진행되고 있으며, 탐지 정확도도 점차 향상되고 있다. 하지만, IoT 환경의 특징인 저 사양 하드웨어, 고차원의 특징, 방대한 트래픽 등으로 인해 탐지성능이 저하되는 문제가 있다. 따라서 본 논문에서는 MQTT(Message Queuing Telementry Transport) 프로토콜 기반의 IoT 환경에서 수집된 데이터셋을 대상으로 주성분 분석(Principal Component Analysis)과 LightGBM을 이용하여 데이터셋 차원을 감소시키고, 공격 클래스를 분류하였다. 실험결과 원본 데이터셋 차원을 주성분 3개(약 9%)로 감소시켰음에도 모든 특징(33개)을 사용한 실험결과와 거의 유사한 성능을 보였다. 또한 기존 연구의 특징 선택을 통한 탐지 모델과 비교하였을 때도 분류성능이 더 우수한 것으로 나타났다.

키워드: 사물인터넷, 주성분 분석, 기계학습, LightGBM, 사물인터넷 공격 탐지

I. Introduction

사물인터넷(IoT, Internet of Things) 기기는 4차 산업혁명, 5G 보급 등으로 인해 실생활, 산업, 의료, 국방 분야 등 전 분야에 걸쳐 급속히 확산 되어왔으며, 2027년에는 IoT 기기의 수가 410억대에 달할 것으로 예상된다[1].

한편, 이러한 IoT 기기의 기하급수적 증가는 엄청난 양의 데이터 증가와 다양한 보안 취약점의 노출로 이어져 사이버 보안 구현을 더욱 어렵게 하고 있다.

이에 최근 다양한 기계학습 기반의 침입 탐지 모델 연구가 이루어지고 있으며, 탐지 정확도는 갈수록 높아지고 있다. 하지만 기계학습 기반 모델의 경우 차원이 큰 대규모 데이터를 대상으로 하는 탐지 및 분류에 있어서 시간 복잡성과 공간 복잡성의 한계에 직면하게 된다.

따라서 본 연구에서는 데이터의 특징을 추출해 차원을 압축하는 기법인 주성분 분석(PCA)과 LightGBM을 이용하여 IoT 네트워크 공격에 대한 탐지 및 분류 효율을 높이는 기법을 제안한다.

실험에 사용된 데이터는 IoT 표준 프로토콜 중 하나로 국방 분야에서도 적용되고 있는 MQTT 프로토콜 환경에서 수집된 MQTTset[2]을 사용하였다.

II. Related Work

IoT 환경에서의 효율적인 공격 탐지를 위해 데이터 차원을 축소하는 연구가 활발히 이루어지고 있다. [3]에서는 비지도 특징 추출 기반으로 고차원 데이터를 효과적으로 압축하는 주성분 분석(Principal Component Analysis)을 활용하여 낮은 연산복잡도에서 높은 성능을 보이는 이상 탐지 기술을 제시하였다.

[4]에서는 MQTTset 데이터를 이용하여 특징 중요도(feature importance) 기반의 특징 선택(feature selection)을 통해 데이터의 차원을 축소하면서 탐지성능을 향상시키는 방안을 제시하였다.

III. The Proposed Scheme

3.1 Data

MQTTset은 33개의 특징을 가지고 있으며 정상 데이터와 5개의 공격 클래스(DoS, SlowIte, Flood, Bruteforce, Malformed)로 구성되어 있다. 학습 데이터셋과 테스트 데이터셋은 70%와 30%로 분할 사용하였다.

3.2 Method

학습 데이터셋에 대하여 주성분 분석을 통해 특징을 추출하고, 추출된 특징을 기반으로 전체 데이터셋의 차원을 감소시켰다. 이후 LightGBM(Light Gradient Boosting Model)을 이용하여 정상 데이터와 5개의 공격 클래스를 분류하였다. 실험과정은 그림 1과 같다.

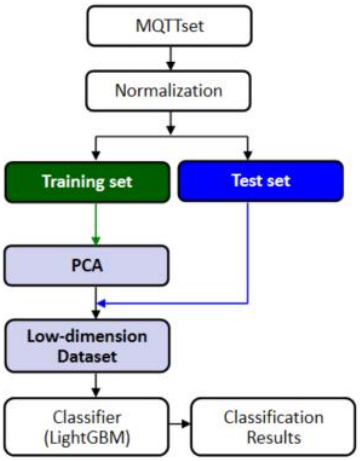

Fig. 1. Flowchart of the proposed Method

3.3 Results

성능 평가지표로는 정확도(accuracy), F1-score를 사용하였다. 실험결과 주성분 3개에서 전체 데이터의 74.53%를 설명할 수 있는 분산도가 측정되었으며, 정확도는 93.56%, F1-score는 0.9343으로 원본 데이터의 특징(33개)을 모두 사용한 결과(정확도 93.98%, F1-score 0.9392) 대비 정확도는 0.42%, F1-score는 0.0049 낮게 측정되었다.

기존 연구[4]에서 제안한 기법을 통해 특징 3개를 선택하여 사용한 실험결과는 정확도 90.02%, F1-score 0.8914로 본 연구에서 제안한 기법이 더 우수한 성능을 나타냄을 확인하였다. 실험결과는 표 1과 같다.

Table 1. Experimental Results

구 분	PC10	PC7	PC5	PC3
분산도	0.9878	0.9421	0.8671	0.7453
정확도	0.9382	0.9380	0.9368	0.9356
F1-score	0.9366	0.9357	0.9355	0.9343

IV. Conclusions

본 연구에서는 MQTTset 데이터에 대하여 주성분 분석과 LightGBM을 이용하여 IoT 환경에서의 효율적인 네트워크 공격 탐지 기법을 제안하였다.

원본 데이터셋 차원을 약 9%로 감소시킨 3개의 주성분으로 실험한 결과 정확도와 F1-score는 원본 데이터의 모든 특징(33개)을 사용한 결과와 유사한 성능을 보였다. 이러한 실험결과를 통해 낮은 시간복잡도와 공간복잡도를 요구하는 IoT 환경에서 제안 기법이 유효함을 확인할 수 있었다.

향후에는 더욱 고차원의 IoT 데이터셋을 이용하여 제안한 기법에 대한 추가적인 연구를 진행할 예정이다.

REFERENCES

[1] Ahmad, Rasheed, and Izzat Alsmadi. "Machine learning approaches to IoT security: A systematic literature review", Internet of Things, Vol. 14, pp. 1-42, June. 2021.

[2] Ivan Vaccari, OrcID, Giovanni Chiola, Maurizio Aiello, OrcID,Maurizio Mongelli, Enrico Cambiaso, “MQTTset, a New Dataset for Machine Learning Techniques on MQTT”, Sensors, Vol 20, 2020.

[3] Hyoseon Kye, and Minhae Kwon, "PCA-Based Low-Complexity Anomaly Detection", The Journal of Korean Institue of Communications and Information Science, Vol. 46, No. 06, pp. 941-955, June. 2021.

[4] Maheshi B. Dissanayake, "Feature Engineering for Cyber-attack detection in Internet of Things", I.J Wireless and Microwave Technologies, pp. 46-54, June 2021.